Kobalos

Deberán leer cada una de las noticias asignadas y responder en un documento de Google Presentations para todas las mesas, las siguientes consignas:

• ¿Qué tipo de amenaza es?
Es un Backdoor-Malware

• ¿Cómo comienza y cómo se propaga esta amenaza?
No se sabe exactamente cómo comenzó y a partir de estos hay algunas posibles teorías basándose en artefactos forenses recopilados sobre cómo Kobalos afectó a los sistemas.

Descubrimos que un ladrón de credenciales SSH estaba presente en forma de un cliente OpenSSH troyanizado. El /usr/bin/ssh
El archivo se reemplazó con un ejecutable modificado que registraba el nombre de usuario, la contraseña y el nombre de host de destino, y los escribió en un archivo encriptado. Por lo tanto, creemos que el robo de credenciales podría ser una de las formas en que Kobalos propaga.

• ¿Hay más de una amenaza aplicada?
No encontraron ningún otro malware, excepto por el ladrón de credenciales SSH.

• ¿Qué solución o medida recomendarían?
Desde una perspectiva de red, es posible detectar Kobalos buscando tráfico que no sea SSH en el puerto atribuido a un servidor SSH. Cuando el backdoor Kobalos se comunica con un operador, no se intercambia ningún banner SSH (SSH-2.0-…), ni desde el cliente ni del servidor.

Sugerimos que para conectarse a servidores SSH configurar antes el doble factor de autenticación (2FA). Kobalos es otro caso en el que el 2FA podría haber mitigado la amenaza, ya que el uso de credenciales robadas parece ser una de las formas en que se puede propagar a diferentes sistemas.